destination platform. Thus, the need for configuring the requesting platform to suit a

particular proxy configuration is eliminated along with the associated overhead. An example

of such a network caching technique is embodied in the Web Content Caching Protocol

(WCCP) provided by Cisco Systems, Inc., a specific embodiment of which is described in *(Now US pat. No. 6,240,461)*

5   copending, commonly assigned, U.S. Patent Application No. 08/946,867 for METHOD   *ko*

AND APPARATUS FOR FACILITATING NETWORK DATA TRANSMISSIONS filed   *4/29/06*

please enter

October 8, 1997, the entirety of which is incorporated herein by reference for all purposes.

        Another specific embodiment of a packet redirection protocol which may be used to

implement such a network caching technique is described in copending, commonly assigned,

10   U.S. Provisional Patent Application No. 60/168,862 for METHOD AND APPARATUS

FOR REDIRECTING NETWORK TRAFFIC filed December 2, 1999, the entirety of which

is incorporated herein by reference for all purposes. According to a specific embodiment

described in that application, the network caches have the capability of determining that

particular redirected packets should be transmitted back to the redirecting router and

15   reinserted into the original traffic flow. This may be done in a manner transparent to the

source or destination of the packets. An example of a case in which packets would need to

be reinserted in the original flow might be where the cache recognizes the source and

destination pairs identified by the packets as corresponding to a connection requiring IP-

based authentication. Another example would be where the cache is overloaded and is

20   currently unable to handle all of the redirected traffic.

        When information in a packet flow between two devices, e.g., a router and a network

cache, is corrupted, it is useful for troubleshooting purposes to examine the sequence of

packets as they are transmitted over the link. One technique for determining the cause of

such corruption involves the insertion of a hub between the two devices and the connection

25   of a network sniffer to the hub. The hub duplicates all the packets in the flow and the sniffer